

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Washington, DC 20554

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date of execution: **February 26, 2008**

Name of Company covered by this certification: **South Central Communications**

Form 499 Filer ID: **821190**

Name of Officer signing: **Brant Barton**


Title of Officer signing: **Chief Executive Officer**

I, **Brant Barton**, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification as Exhibit 1 is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by a company at either state commission, the court system, or at the Commission against data brokers) against data brokers in the past year

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed  _____

cc: Telecommunications Consumers Division, Enforcement Bureau
Best Copy and Printing, Inc.

SOUTH CENTRAL UTAH TELEPHONE

STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES

I. Customer Proprietary Network Information ("CPNI")

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

II. Use and Disclosure of CPNI Is Restricted

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; and (4) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access the Company's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

III. Protection of CPNI

1. The Company will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.
2. Since December 8, 2007, the Company retains all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.
3. Since December 8, 2007, Company employees authenticate requests for CPNI in the following manner. Company employees must: (a) be furnished the customer's pre-established password (or correct answers to the back-up "shared secret" combinations); (b) send the requested information to the customer's postal or electronic "address of record" (c) call the customer back at the customer's "telephone number of record" with the requested information or (d) at its retail locations the customer presents a valid photo ID and the photo ID matches the name on the account.
4. The Company has adopted a policy that it does not and will not use, disclose or permit access to CPNI by an affiliate.
5. When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after the Company authenticates the customer.

Since December 8, 2007, if the customer is able to provide to the Company during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call) without Company assistance, then the Company may take routine customer service actions related to such information. (However, under this circumstance, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.)

6. The Company has adopted a policy that it does not and will not use, disclose, or permit access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing).

7. The Company's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

8. The Company's employees and agents may use CPNI without customer approval to protect the Company's rights or property, and to protect users and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived.

Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section must be expressly approved in advance and in writing by the Company's CPNI Compliance Officer.

9. The Company's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers. Nor may the Company's employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

10. Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

11. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.

12. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

13. The Company may permit its customers to establish online accounts, but must require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account. Since December 8, 2007, passwords may **NOT** be based upon readily obtainable biographical information (*e.g.*, the customer's name, mother's maiden name, social security number or date of birth) or account information (*e.g.*, the customer's telephone number or address).

14. Since December 8, 2007, the Company will notify customers of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (a) a Company call or voicemail to the customer's telephone number of record; (b) a Company text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record or email of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

15. Since December 8, 2007, the Company must provide an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.

As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, the Company must provide electronic notification of such breach to the United States Secret Service and to the Federal Bureau of Investigation via a central reporting facility accessed through a link maintained by the FCC at <http://www.fcc.gov/eb/cpni>.

16. The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring Company employees, agents, independent contractors and joint venture partners to notify the CPNI Compliance Officer immediately by voice, voicemail or email of any suspicious or unusual activities requesting a customer's call detail information or other CPNI

17. The Company and its authorized employees may use CPNI to provide call location information regarding mobile users in emergency situations involving a substantial threat to human life or safety.

IV. CPNI Compliance Officer

In addition to the specific matters required to be reviewed and approved by the Company's CPNI Compliance Officer, employees and agents, independent contractors and joint venture partners are strongly encouraged to bring any and all other questions, issues or uncertainties regarding the use, disclosure, or access to CPNI to the attention of the Company's CPNI Compliance Officer for appropriate investigation, review and guidance. The extent to which a particular employee or agent brought a CPNI matter to the attention of the CPNI Compliance Officer and received appropriate guidance is a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure or access to CPNI.

V. Disciplinary Procedures

The Company has informed its employees and agents, independent contractors and joint venture partners that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important.

Violation by Company employees or agents of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious).

Violation by Company independent contractors or joint venture partners of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training and termination of the contract).